UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/813,024	03/21/2001	Takeshi Shimoyama	826.1715	2742

21171 7590 10/22/2004

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
HUA, LY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/813,024	SHIMOYAMA ET AL.	
	Examiner	Art Unit	
	Ly V. Hua	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☑ Claim(s) 1-25 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☑ Claim(s) 1-25 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☑ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4/16/01, 3/12/04
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. Figure 1A to 1F should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.121(d)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

   . The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. With regard to claim 1:
   a. Even thought the abbreviations SPN, S and F are well known in the art, the appearances of those abbreviations for the first time in a claim in short form do not make clear as to what they are. The applicant is requested to associate each of the abbreviations with its long form where they are presented for the first time in the claim.
      i The abbreviation "SPN" cannot be understood from the recitation of the claim.
      ii The abbreviation "S" cannot be understood from the recitation of the claim.
      iii The abbreviation "F" cannot be understood from the recitation of the claim.
   b. The description of what the value indicates does not make it clear as to what the outputting unit is like structurally in term of hardware component of the output unit of the computing apparatus.
   c. The description of the how the input bit numbers is obtained prior to being received by the input unit of the computing apparatus does not make it clear as to what the input unit is like structurally in term of hardware component of the input unit of the computing apparatus.
   d. It is not clear as to how the output unit operate so that it's output value A_T that can indicate the probability of the linear-converting-unit.
   e. The antecedent basis for the term "which" is not clear.
      i Notice that:
         (1) It is not clear as to whether it is referred to a single S box or all of the plurality of S boxes.
         (2) The equivalencies among numbers are confusing among the plurality and divided bit numbers and among the input but numbers and the output bit numbers.
   f. Applicant's way of presenting the claimed computer apparatus is so confusing that the structure of the computer apparatus cannot be seen from the recitation of the claim itself.
   g. *It is not clear how the input and output bit number of the plurality of S boxes are made equivalent to the divided bit numbers in order for the applicant to present that the input and output* bit numbers of which plurality of S boxes are equivalent to the divided bit numbers.
   h. It is not clear whether the second constituent the computing apparatus should be read to be "a value" (which has the function of indicating) or "a … outputting unit" (which has the function outputting).

5. With regard to claims 2-10:
   a. These claims depend on claim 1 and thus inherit the problems of indefiniteness therefrom.

6. With regard to claim 11:
   a. Even thought the abbreviations SPN, S and F are well known in the art, the appearances of those abbreviations for the first time in a claim in short form do not make clear as to what they are. The applicant is requested to associate each of the abbreviations with its long form where they are presented for the first time in the claim.

i The abbreviation "SPN" cannot be understood from the recitation of the claim.
ii The abbreviation "S" cannot be understood from the recitation of the claim.
iii The abbreviation "F" cannot be understood from the recitation of the claim.

b. This claim is directed to a method, but the steps recited appear to have no interaction so as to produce a result of the method.
c. The purpose for which the method is performed is not clear.

7. With regard to claims 12 and 13:
   a. These claims depend on claim 1 and thus inherit the problems of indefiniteness therefrom.

8. With regard to claim 14:
   a. Even thought the abbreviations SPN, S and F are well known in the art, the appearances of those abbreviations for the first time in a claim in short form do not make clear as to what they are. The applicant is requested to associate each of the abbreviations with its long form where they are presented for the first time in the claim.
      i The abbreviation "SPN" cannot be understood from the recitation of the claim.
      ii The abbreviation "S" cannot be understood from the recitation of the claim.
      iii The abbreviation "F" cannot be understood from the recitation of the claim.
   b. That which is performed by the computer as is caused by the program is not clear.
   c. That which comprises the "receiving ..." and the "outputting ..." is not clear.

9. With regard to claim 15:
   a. Even thought the abbreviation SPN, is well known in the art, the appearance of it for the first time in a claim in short form does not make clear as to what they are. The applicant is requested to associate it with its long form where it is presented for the first time in the claim.
      i The abbreviation "SPN" cannot be understood from the recitation of the claim.

10. With regard to claims 16-18:
    a. These claims depend on claim 15 and thus inherit the problems of indefiniteness therefrom.

11. With regard to claim 19:
    a. This claim is a method claim, but the steps (of the method) have not been clearly recited to show how the steps are related to each other for bring forth a result after performing the steps of the method. How the two steps interact with each other is not clear.
    b. Even thought the abbreviation SPN, is well known in the art, the appearance of it for the first time in a claim in short form does not make clear as to what they are. The applicant is requested to associate it with its long form where it is presented for the first time in the claim.
       i The abbreviation "SPN" cannot be understood from the recitation of the claim.

12. With regard to claim 20:
    a. It is not clear whether the first data conversion uses the Feistel structure or the SPN structure.
       i This is because Claim 19 states that it uses Feistel structure, but then in claim 20 it is stated that the first data conversion uses the SPN structure.
       ii The applicant is to avoid such confusion.
    b. The phrase "wherein in the first data conversion using the SPN structure" lacks antecedent basis since no SPN structure has been used by the first data conversion.
    c. The word "liner" at line 22 appears to be in error.
    d. The clause "liner conversion ... are executed" appears to be not idiomatic (due do subject-verb number agreement problem).

13. With regard to claims 21-22:
    a. These claims depend on claim 19 and thus inherit the problems of indefiniteness therefrom.

14. With regard to claim 22:

a. This claim depends on claim 20 and thus inherits the problems of indefiniteness therefrom.

15. With regard to claim 23:
    a. Even thought the abbreviation SPN, is well known in the art, the appearance of it for the first time in a claim in short form does not make clear as to what they are. The applicant is requested to associate it with its long form where it is presented for the first time in the claim.
        i The abbreviation "SPN" cannot be understood from the recitation of the claim.

16. With regard to claim 24:
    a. Claim 24 has the same problems of indefiniteness as those of claim 1. Notice that claim 24 and claim 1 are presented in the same way.

17. With regard to claim 25:
    a. Even thought the abbreviation SPN, is well known in the art, the appearance of it for the first time in a claim in short form does not make clear as to what they are. The applicant is requested to associate it with its long form where it is presented for the first time in the claim.
        i The abbreviation "SPN" cannot be understood from the recitation of the claim.
    b. The objects being combined by the combining step are not clear.
        i The applicant is to avoid reciting the combinations of steps in this manner since when the combining is done and when the executing is done are not clear.
    c. The Applicant is to recite this claim (and other apparatus claims and method claims) in the formats that are of U.S. patent claim format.

18. The above are examples of problems of indefiniteness in the claims. The applicant is also to review, detect and correct any other ones if found.

Claim Rejections - 35 USC § 102

19. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:
A person shall be entitled to a patent unless –

.(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

.(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

.(c) he has abandoned the invention.

.(d) the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months before the filing of the application in the United States.

.(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

.(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Note: The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

.(f) he did not himself invent the subject matter sought to be patented.

.(g)(1) during the course of an interference conducted under section 135 or section 291, another inventor involved therein establishes, to the extent permitted in section 104, that before such person's invention thereof the invention was made by such other inventor and not abandoned, suppressed, or concealed, or (2) before such person's invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. In determining priority of invention under this subsection, there shall be considered not only the respective dates of conception and reduction to practice of the invention, but also the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.

20. Claims 1, 11, 14, 15, 19, 23, 24 and 15 are rejected under 35 U.S.C. 102(f) as being not being invented (as claimed) by the applicant, but are of applicant's admitted art (as the way in which the claims are presented. with repletion of indefiniteness problems).

This table shows claims 1 and 24 in parallel for ease of seeing the similarities between them.

21. 24. A computing apparatus	22. 1. A computing apparatus
a. using i SPN structure (1) having (a) a plurality of S boxes and (b) a linear converting unit in an F function,	a. using SPN structure i having (1) a plurality of S boxes and (2) a linear converting unit (a) in an F function,
b. comprising:	b. comprising:
i set of bit numbers inputting means (1) for receiving (a) an input (i) of a set T= $\{t_1, t_2, t_3, \ldots, t_\tau\}$ (ii) of bit numbers (iii) obtained 1) by unequally dividing all bit numbers of input data to be given to the computing apparatus;	i a set of bit numbers inputting unit (1) receiving (a) an input (i) of a set T=$\{t_1, t_2, t_3, \ldots, t_\tau\}$ (ii) of bit numbers 1) obtained a) by unequally dividing all bit numbers of input data to be given to the computing apparatus; and
ii an value indicating existence probability of linear converting unit outputting means (1) for outputting (a) a value A_T (i) indicating 1) an existence **probability** a) of an appropriate linear converting unit b) corresponding to i) a plurality of S boxes of which input and output bit numbers are equivalent to the divided bit numbers.	ii a value indicating existence probability of linear converting unit outputting unit (1) outputting (a) a value A_T (i) indicating 1) an existence probability a) of an appropriate linear converting unit b) corresponding to i) a plurality of S boxes of which input and output bit numbers are equivalent to the divided bit numbers.

23. As to claims 1 and 24:
    a. Preliminary matters:
        i How the bit numbers of the set T is obtained appears to be not of the computing apparatus since the obtaining of the bit numbers appears to have occurred outside the computer apparatus.
            (1) The merit of the input unit will not be based on how the input (it receives) has been obtained since the obtaining of the input (as presented in the claim) is not done by of the computing apparatus, (which computing apparatus just has an input unit that receives the input).
        ii The recitation of the probability of the converting unit to be corresponding with the S-boxes appears to have nothing to do with the output unit, since the relationship between the indication and the function of the output unit's function to output the output is not clear. In effect, it is not clear as to how the value A_T is derived so that it can possibly indicate such probability.
            (1) Due to this problem of vagueness, patentability weight cannot be given to the meaning of the value of A_T.
                (a) (As it is, the claim is directed to an apparatus, the Examiner looks for the structural/configuration of the output unit, rather than what its output indicate, unless the specific way in which the value A_T is derived by the specific concrete circuitry/elements).
    b. The above preliminary matters, the examiner gives merits to the following (as elements of a claim that is directed to a computing apparatus):
        i a computing apparatus comprising:
            (1) an input unit,
                (a) which input unit has a function of receiving for inputting an input, and
            (2) an output unit,
                (a) which output unit has a function of outputting for outputting an value.
    c. With respect to what can be given merit on, the examiner presents:
        i Applicant's admitted prior art teaches [e.g. Figure 1A]:
            (1) 1. A computing apparatus [Figure 1A]
                (a) using SPN structure [i.e., element F51A (detailed by Figure 1B)]
                    (i) having
                        1) a plurality of S boxes [i.e., element S63 (the combination of which is called non-linear converting unit)] and
                        2) a linear converting unit [i.e., element P64]
                            a) in an F function [i.e.., the function of element F51 shown back in Figure 1A],
                (b) comprising:
                (c) a set of bit numbers inputting unit [i.e., the line for inputting the input P having (e.g., 64) bits which are divided into two sets, each of which set has 32 bits, one set going to the right side of Figure 1A and the other set going to the left side of Figure 1A] receiving
                    (i) an input [i.e., input P which has 64 bits as shown]
                        1) of a set T={t1, t2, t3 , . . ., tr} --- [i.e., r=64 as shown]
                            a) of bit numbers
                                i) obtained ~~by unequally dividing all bit numbers of input data to be given to the computing apparatus~~; and
                (d) a ~~value indicating existence probability of linear converting unit~~ outputting unit [i.e., the line for outputting the output C having (e.g., 64) bits which are merged from two sets, each of which set has 32 bits, one set comes from the right side of Figure 1A and the other set comes from the left side of Figure 1A] outputting
                    (i) a value AT I[i.e., output C which has 64 bits as shown] .
                        ~~1) indicating~~
                            ~~a) an existence probability of an appropriate linear converting unit corresponding to a plurality of S boxes,~~
                                {1} of which input and output bit numbers *of which S boxes* are equivalent to the divided bit numbers .
    d. The examiner strikes through the texts as shown because they cannot be understood as presented above in the rationales for rejecting the claims as being indefinite under 35 USC 112, second paragraph.
        i To prevent these claims from being rejected in this manner, the applicant is to clearly recite the claim in a manner that can be understood with ease and without confusion. The Applicant is to recite this claim (and other apparatus claims and method claims) in the formats that are of U.S. patent claim format.

This table shows claims 1 and 11 in parallel for ease of seeing the similarities between them.

24. 1. A computing apparatus	25. 11. A computation method
a. using SPN structure	a. using SPN structure
i having	i having
(1) a plurality of S boxes and	(1) a plurality of S boxes and
(2) a linear converting unit	(2) a linear converting unit
(a) in an F function,	(a) in an F function,
b. comprising:	b. comprising:
c. a set of bit numbers inputting unit receiving	i receiving
i an input	(1) an input
(1) of a set $T=\{t_1, t_2, t_3, \ldots, t_\tau\}$	(a) of a set $T=\{t_1, t_2, t_3, \ldots, t_\tau\}$
(a) of bit numbers	(i) of bit numbers
(i) obtained by	1) obtained by
1) unequally dividing all bit numbers of input data to be given to the computing apparatus; and	a) unequally dividing all bit numbers of input data to be given; and
d. a _____ outputting unit outputting	ii outputting
i a value A_T	(1) a value A_T
(1) indicating	(a) indicating
(a) an existence probability	(i) an existence probability
(i) of an appropriate linear converting unit	1) of an appropriate linear converting unit
1) corresponding to	2) corresponding to
a) a plurality of S boxes	a) a plurality of S boxes
{1} ~~of which~~ input and output bit numbers *of which S boxes* are equivalent to the divided bit numbers.	i) of which input and output bit numbers are equivalent to the divided bit numbers.

26. As to claim 11:
    a. Claim 11 has limitations that are similar to those of claim 1, and thus is similarly rejected with the same rationales applied against claim 1.
        i The steps of claim 11 are the function of the elements of either claim 1 or claim 24.

This table shows the claims 11 and 14 in parallel for easy of seeing the similarities between them.

27. 11. A computation method a. using SPN structure i having (1) a plurality of S boxes and (2) a linear converting unit (a) in an F function, b. comprising: i receiving (1) an input (a) of a set T= $\{t_1, t_2, t_3, \ldots, t_r\}$ (i) of bit numbers 1) obtained by a) unequally dividing all bit numbers of input data to be given; and ii outputting (1) a value A_T (a) indicating (i) an existence probability 1) of an appropriate linear converting unit 2) corresponding to a) a plurality of S boxes i) of which input and output bit numbers are equivalent to the divided bit numbers.	28. 14. A computer-readable portable recording medium a. used i by a computer (1) executing (a) a computation process (i) using 1) SPN structure having a) a plurality of S boxes and b) a linear converting unit in an F function, b. storing a program for causing the computer to perform, c. comprising: i receiving (1) an input (a) of a set T= $\{t_1, t_2, t_3, \ldots, t_r\}$ of bit numbers 1) obtained by a) unequally dividing all bit numbers of input data to be given; and ii outputting (1) a value A_T (a) indicating (i) an existence probability 1) of an appropriate linear converting unit 2) corresponding to a) a plurality of S boxes i) of which input and output bit numbers are equivalent to the divided bit numbers.

29. As to claim 14:
    a. Claim 14 has limitations that are similar to those of claim 11 and thus in turn similar to those of either claim 1 or 24, and thus is similarly rejected with the same rationales applied against claim 1.
    b. It is inherent
        i that a computer
            (1) that uses Applicant's admitted prior art
            (2) has:
                (a) a portable computer-readable recording medium
                    (i) being used
                        1) by the computer
                            a) to executes computation of receiving data input and
                            b) that sets a computation result for the input data as a data output; and
                    (ii) storing
                        1) a program
                            a) causing the computer (implementing the apparatus of either claim 15 or claim 25) to perform
        ii so as to carry out the method of claim 19 performed by the apparatus of either claim 15 or claim 25.

This table shows claims 25 and 15 in parallel for ease of seeing the similarities among them.

30. 25. A computing apparatus a. in which i Feistel structure and SPN structure (1) are combined, b. for i receiving (1) a data input, and ii setting (1) a computation result for the data input (2) as a data output, c. comprising: i at least one first data converting means (1) for performing (a) data conversion using the Feistel structure; and ii at least one second data converting means (1) for performing (a) data conversion using the SPN structure, d. wherein i said first data converting means and said second data converting means (1) are continuously combined (a) between (i) the data input and (ii) the data output.	31. 15. A computing apparatus a. in which i Feistel structure and SPN structure (1) are (a) combined, b. receiving i data input and ii setting (1) a computation result for the data input (2) as a data output, c. wherein i at least one first data converting units (1) that perform (a) data conversion using the Feistel structure, and ii at least one second data converting units (1) that perform (a) data conversion using the SPN structure iii are continuously combined (1) between (a) the data input and (b) the data out.

32. As to claims 25 and 15:

a. Applicant's admitted prior art teaches a computing apparatus [i.e., Figure 1A]
   i in which
      (1) Feistel structure [e.g., Figure 1A] and SPN structure [element F of Figure 1A, detailed by Figure 1B]
         (a) are combined [i.e., each of the elements F of Figure 1A is implemented with the structure of Figure 1B],
   ii for
      (1) receiving [at the top of the structure of Figure 1A]
         (a) a data input [of e.g., 64 bits], and
      (2) setting [at the bottom of the structure of Figure 1A]
         (a) a computation result [e.g., of 64 bits at the bottom of the structure of Figure 1A] for the data input
         (b) as a data output [i.e., output C which is of, e.g., 64 bits],
   iii comprising:
      (1) at least one first data converting means [i.e., the structure of Figure 1A]
         (a) for performing
            (i) data conversion using the Feistel structure [as Figure 1A is a Feistel Structure]; and
      (2) at least one second data converting means [i.e., the structure of Figure 1B]
         (a) for performing
            (i) data conversion using the SPN structure [as Figure 1B is a SPN structure],
   iv wherein
      (1) said first data converting means and said second data converting means
         (a) are continuously combined [as shown in Figure 1A and Figure 1B]
            (i) between
               1) the data input [P] and
               2) the data output [C].

This table shows claims 25, 19 and 23 in parallel for ease of seeing the similarities among them.

33. 25. A computing apparatus	34. 19. A computation method	35. 23. A portable computer-readable recording medium
a. in which i Feistel structure and SPN structure (1) are combined,	a. in which i Feistel structure and SPN structure (1) are combined,	a. being used i for a computer (1) that executes (a) computation of receiving data input and (2) that sets (a) a computation result for the input data (b) as a data output, and
b. for i receiving (1) a data input, and ii setting (1) a computation result for the data input (2) as a data output,	b. receiving i a data input and ii setting (1) a computation result for the data input (2) as a data output,	b. storing i a program (1) causing (a) the computer (i) to perform,
c. comprising: i at least one first data converting means (1) for performing (a) data conversion using the Feistel structure; and ii at least one second data converting means (1) for performing (a) data conversion using the SPN structure,	c. wherein i [two pieces (1) including] (a) at least one piece of first data conversion (i) that performs 1) data conversion using the Feistel structure and (b) at least one piece of second data conversion (i) that performs 1) data conversion using the SPN structure (2) are combined (a) to be executed (i) between 1) the data input and 2) the data output.	c. comprising: i combining and ii executing (1) at least one piece (a) of first data conversion (i) that performs 1) data conversion using Feistel structure; and (2) at least one piece (a) of second data conversion (i) that performs 1) data conversion using SPN structure (3) between (a) the data input and (b) the data output.
d. wherein i said first data converting means and said second data converting means (1) are continuously combined (a) between (i) the data input and (ii) the data output.		

36. As to claims 19 and 23:
    a. Each of the claims 19 and 23 has limitations that are similar to those of claim 25, and thus is similarly rejected with the same rationales applied against claim 25.
    b. With regard to claim 19:
        i The teach of Applicant's admitted prior art teach each of the apparatuses of claims 25 and 15, which in turn teaches the method of claim 19 since the method of claim 19 is carried out by each of the apparatuses of claims 25 and 15.
    c. With respect to claim 23:
        i It is inherent
            (1) that a computer
                (a) that uses Applicant's admitted prior art
                (b) has:
                    (i) a portable computer-readable recording medium
                        1) being used
                            a) by the computer
                                i) to executes computation of receiving data input and
                                ii) that sets a computation result for the input data as a data output; and
                        2) storing
                            a) a program
                                i) causing the computer (implementing the apparatus of either claim 15 or claim 25) to perform
            (2) so as to carry out the method of claim 19 performed by the apparatus of either claim 15 or claim 25.

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ly V. Hua whose telephone number is (703) 305-9684. The examiner can normally be reached on Monday to Friday from 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vu Kim, can be reached on 703-305-4303. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

39. The applicant is hereby notified that:
    a. TC 2100 will be moved to Carlyle in October 2004.
    b. The new phone number for TC 2100 receptionist is (571) 272-2100.
    c. The examiner's new contact phone number will be (571) 272-3853.

Ly V. Hua
Primary Examiner
Art Unit 2135

Lvh
October 1, 2004